# BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

## IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.**

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10283320 A**

(43) Date of publication of application: **23 . 10 . 98**

(51) Int. Cl **G06F 15/00**
**G06F 9/06**
**G06F 19/00**
**G07F 7/08**

(21) Application number: **10005411**

(22) Date of filing: **14 . 01 . 98**

(30) Priority: **05 . 02 . 97 JP 09 22256**

(71) Applicant: **N T T DATA:KK**

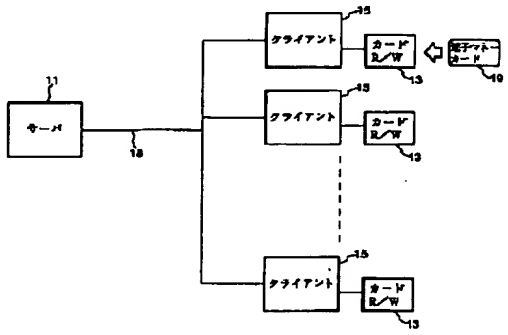
(72) Inventor: **NAKAJIMA YUSAKU**
**MORI HIROYOSHI**

(54) **PRIVACY SYSTEM AND SECRET PROGRAM MANAGEMENT SYSTEM AND RECORDING MEDIUM**

(57) Abstract:

PROBLEM TO BE SOLVED: To increase the level of security, and to attain realization by general hardware.

SOLUTION: A client 15 reads user information stored in an electronic money card 19 mounted on a card reader/writer, and transmits it to a server 11. The server 11 receives the user information from the client 15, and transmits an IC card writing program being a privacy program to the client 15. The client 15 executes the received IC card writing program, deletes the program after completing the execution, and transmits a deletion completion telegraphic message to the server 11. The server 11 waists for the deletion completion telegraphic message from the client 15 in a prescribed time after transmitting the IC card writing program to the client 15. When the server 11 does not receive the deletion completion telegraphic message in the prescribed time, the server 11 specifies an unauthorized user from the user information received from the client 15.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－283320

(43)公開日　平成10年(1998)10月23日

| (51)Int.Cl.[6] | | 識別記号 | FI | | |
|---|---|---|---|---|---|
| Ｇ０６Ｆ | 15/00 | ３３０ | Ｇ０６Ｆ | 15/00 | ３３０Ａ |
| | 9/06 | ５５０ | | 9/06 | ５５０Ｚ |
| | 19/00 | | | 15/30 | Ｃ |
| Ｇ０７Ｆ | 7/08 | | | | ３５０Ａ |
| | | | Ｇ０７Ｆ | 7/08 | Ｚ |

審査請求　未請求　請求項の数15　ＯＬ　（全 14 頁）

(21)出願番号　特願平10－5411

(22)出願日　平成10年(1998)１月14日

(31)優先権主張番号　特願平9－22256

(32)優先日　平９(1997)２月５日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号

(72)発明者　中島　雄作
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

(72)発明者　森　啓悦
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

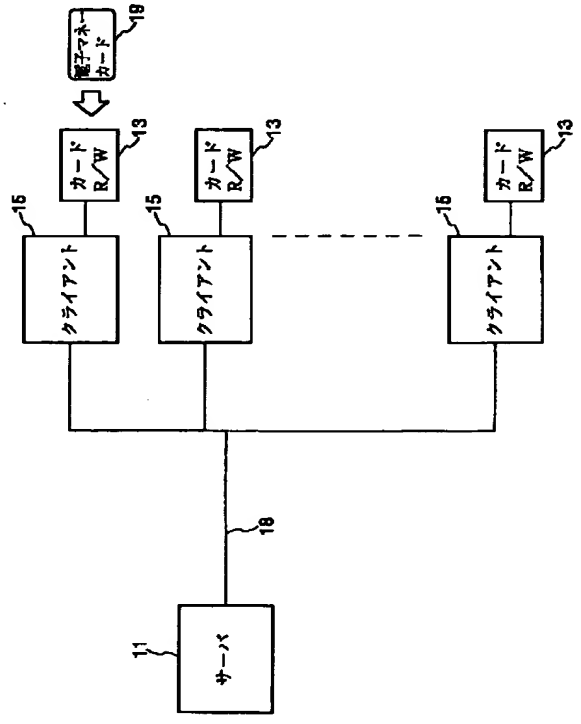
(74)代理人　弁理士　木村　満

(54)【発明の名称】　セキュリティシステム、機密プログラム管理方法及び記録媒体

(57)【要約】

【課題】　セキュリティのレベルが高く、汎用的なハードウェアで実現可能なセキュリティシステム、機密プログラム管理方法及び記録媒体を提供する。

【解決手段】　クライアント１５は、カードＲ／Ｗ１３に装着された電子マネーカード１９に記憶されている利用者情報を読み出し、サーバ１１に送信する。サーバ１１は、クライアント１５から利用者情報を受信すると、機密プログラムであるＩＣカード書込プログラムをクライアント１５に送信する。クライアント１５は、受信したＩＣカード書込プログラムを実行し、実行完了後、そのプログラムを削除すると共に、削除完了電文をサーバ１１に送信する。サーバ１１は、ＩＣカード書込プログラムをクライアント１５に送信した後、クライアント１５からの削除完了電文を所定時間待つ。削除完了電文を所定時間内に受信しない場合、サーバ１１は、クライアント１５から受信した利用者情報より不正者を特定する。



1

【特許請求の範囲】

【請求項１】サーバと、該サーバに接続された複数のクライアントと、を備えるクライアントサーバシステムにおいて、

前記サーバは、

機密情報を含む機密プログラムを記憶する機密プログラム記憶手段と、

前記クライアントからの要求に応じて、前記機密プログラム記憶手段に記憶されている前記機密プログラムを要求元の前記クライアントに送信する手段と、を備え、

前記クライアントは、

前記機密プログラムを前記サーバに要求する要求送信手段と、前記機密プログラムを受信する受信手段と、前記受信手段により受信された前記機密プログラムを記憶する記憶手段と、前記記憶手段により記憶された前記機密プログラムを実行する実行手段と、前記機密プログラム実行後、該機密プログラムを前記記憶手段から削除する削除手段と、を備える、

ことを特徴とするセキュリティシステム。

【請求項２】前記クライアントは、前記機密プログラムへのアクセスに関する排他制御を行うロック制御手段と、前記記憶手段により前記機密プログラムが記憶された際に前記ロック制御手段に該機密プログラムへの排他制御を指示するロック指示手段と、前記実行手段による前記機密プログラムの実行終了後、前記ロック制御手段に該機密プログラムへの排他制御の解除を指示するロック解除指示手段と、を備え、

前記クライアントの前記削除手段は、前記ロック解除指示手段による指示に応じて前記ロック制御手段により前記機密プログラムに関する排他制御が解除された後、該機密プログラムを前記記憶手段から削除する手段を備える、

ことを特徴とする請求項１に記載のセキュリティシステム。

【請求項３】前記クライアントは、少なくとも前記ロック解除指示手段及び前記削除手段による一連の手続が完了するまでの間、タスクの切り替えを禁止する手段をさらに備える、

ことを特徴とする請求項２に記載のセキュリティシステム。

【請求項４】前記クライアントは、前記削除手段による前記機密プログラムの削除後、該機密プログラムのファイル名と同一のファイル名のダミーファイルを作成して記憶するダミーファイル作成手段と、前記作成されたダミーファイルを削除するダミーファイル削除手段と、をさらに備える、

ことを特徴とする請求項２に記載のセキュリティシステム。

【請求項５】前記クライアントは、少なくとも前記ロック解除指示手段、前記削除手段、前記ダミーファイル作

2

成手段及び前記ダミーファイル削除手段による一連の手続が完了するまでの間、タスクの切り替えを禁止する手段をさらに備える、

ことを特徴とする請求項４に記載のセキュリティシステム。

【請求項６】前記クライアントの前記削除手段は、前記機密プログラムの削除後、削除の完了を示す削除完了電文を前記サーバに送信する手段を備え、

前記サーバは、前記機密プログラムの送信先の前記クライアントから前記削除完了電文を該機密プログラム送信時から所定時間内に受信したか否かを判別する判別手段と、前記削除完了電文を前記所定時間内に受信しなかったと判別された場合、不正検出を通知する手段と、を備える、

ことを特徴とする請求項１乃至５のいずれか１項に記載のセキュリティシステム。

【請求項７】前記クライアントは、該クライアントの利用者を特定する利用者情報を取得する取得手段を備え、

前記クライアントの前記要求送信手段は、前記機密プログラムの要求を前記取得手段により取得された前記利用者情報と共に送信する手段を備え、

前記サーバは、前記判別手段により、前記削除完了電文を前記所定時間内に受信しなかったと判別された場合、前記クライアントから受信した前記利用者情報から不正者を特定し、通知する手段を備える、

ことを特徴とする請求項６に記載のセキュリティシステム。

【請求項８】機密プログラムを該機密プログラム保存用の第１の端末に格納するステップと、

前記機密プログラムを実行する第２の端末に前記第１の端末に記憶されている該機密プログラムを転送する転送ステップと、

前記転送ステップにより前記機密プログラムが転送された前記第２の端末において、該機密プログラムを実行し、実行終了後、該機密プログラムを削除する削除ステップと、

を備え、前記機密プログラムの保存と実行を別個の端末で実行することを特徴とする機密プログラム管理方法。

【請求項９】該機密プログラム管理方法は、

前記第２の端末に前記機密プログラムが記憶された際に、該機密プログラムへのアクセスに関する排他制御を行うロックステップと、

前記第２の端末における前記機密プログラムの実行終了後、該機密プログラムへの排他制御を解除するロック解除ステップと、を備え、

前記削除ステップは、前記ロック解除ステップにより前記機密プログラムに関する排他制御が解除された後、該機密プログラムを前記第２の端末から削除するステップを備える、

ことを特徴とする請求項８に記載の機密プログラム管理

方法。

【請求項１０】該機密プログラム管理方法は、

前記第２の端末に前記機密プログラムが記憶された際に、該機密プログラムへのアクセスに関する排他制御を行うロックステップと、

前記第２の端末における前記機密プログラムの実行終了後、該機密プログラムへの排他制御を解除するロック解除ステップと、を備え、

前記削除ステップは、前記ロック解除ステップにより前記機密プログラムに関する排他制御が解除された後、該機密プログラムを前記第２の端末から削除するステップを備え、

該機密プログラム管理方法は、前記削除ステップによる前記機密プログラムの削除後、該機密プログラムのファイル名と同一のファイル名のダミーファイルを作成記憶するステップと、前記作成されたダミーファイルを削除するステップと、をさらに備える、

ことを特徴とする請求項８に記載の機密プログラム管理方法。

【請求項１１】前記削除ステップにより前記機密プログラムが削除された後、削除の完了を前記第１の端末に通知する通知ステップと、

前記第１の端末が、前記通知ステップによる削除の完了の通知を、前記転送ステップによる前記機密プログラムの転送時から所定時間内に受信したか否かを判別する判別ステップと、

前記第１の端末が前記削除の完了の通知を前記所定時間内に受信していないと判別された場合、不正の検出を通知するステップと、

を更に備えることを特徴とする請求項８乃至１０のいずれか１項に記載の機密プログラム管理方法。

【請求項１２】前記転送ステップにより前記機密プログラムが転送された前記第２の端末において、該第２の端末の利用者を特定する利用者情報を取得する取得ステップと、

前記取得ステップより取得された前記利用者情報を前記第１の端末に送信するステップと、

前記判別ステップにより、前記第１の端末が前記削除の完了の通知を前記所定時間内に受信していないと判別された場合、前記利用者情報から不正者を特定し、通知するステップと、

を更に備えることを特徴とする請求項１１に記載の機密プログラム管理方法。

【請求項１３】コンピュータを、

機密情報を含む機密プログラムを要求する要求手段、

前記機密プログラムを受信する受信手段、

前記受信手段により受信された前記機密プログラムを記憶する記憶手段、

前記記憶手段により記憶された前記機密プログラムを実行する実行手段、



前記機密プログラム実行後、該機密プログラムを前記記憶手段から削除する削除手段、

として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１４】コンピュータを、

機密情報を含む機密プログラムを要求する要求手段、

前記機密プログラムを受信する受信手段、

前記受信手段により受信された前記機密プログラムを記憶する記憶手段、

前記機密プログラムへのアクセスに関する排他制御を行うロック制御手段、

前記記憶手段により前記機密プログラムが記憶された際に前記ロック制御手段に該機密プログラムへの排他制御を指示するロック指示手段、

前記記憶手段により記憶された前記機密プログラムを実行する実行手段、

前記実行手段による前記機密プログラムの実行終了後、前記ロック制御手段に該機密プログラムへの排他制御の解除を指示するロック解除指示手段、

前記ロック解除指示手段による指示に応じて前記ロック制御手段により前記機密プログラムに関する排他制御が解除された後、該機密プログラムを前記記憶手段から削除する削除手段、

として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１５】コンピュータを、

機密情報を含む機密プログラムを要求する要求手段、

前記機密プログラムを受信する受信手段、

前記受信手段により受信された前記機密プログラムを記憶する記憶手段、

前記機密プログラムへのアクセスに関する排他制御を行うロック制御手段、

前記記憶手段により前記機密プログラムが記憶された際に前記ロック制御手段に該機密プログラムへの排他制御を指示するロック指示手段、

前記記憶手段により記憶された前記機密プログラムを実行する実行手段、

前記実行手段による前記機密プログラムの実行終了後、前記ロック制御手段に該機密プログラムへの排他制御の解除を指示するロック解除指示手段、

前記ロック解除指示手段による指示に応じて前記ロック制御手段により前記機密プログラムに関する排他制御が解除された後、該機密プログラムを前記記憶手段から削除する削除手段、

前記削除手段による前記機密プログラムの削除後、該機密プログラムのファイル名と同一のファイル名のダミーファイルを作成記憶するダミーファイル作成手段、

前記作成されたダミーファイルを削除するダミーファイル削除手段、

として機能させるためのプログラムを記録したコンピュ

ータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、機密性の高いプログラムを有するコンピュータシステムを、汎用的なハードウェアで実現可能なセキュリティシステム、機密プログラム管理方法及び記録媒体に関する。

【０００２】

【従来の技術】高いレベルのセキュリティが必要とされるコンピュータシステムの一例として、金銭的価値を有する電子マネーをＩＣカードに格納して使用する電子マネーシステムが考えられる。

【０００３】このような電子マネーシステムでは、ＩＣカードへの電子マネーの不正な書き込み等を防止するため、機密性の高い情報（例えば、ＩＣカードへアクセスするためのパスワード）を含むプログラムは、第三者により容易に取得されないよう、強化されたハードウェアに記憶されることが望ましい。また、第三者がその機密性の高いプログラムにアクセスできないよう、利用者のオペレーションを制限することが望ましい。

【０００４】また、そのようにして機密性の高い情報を強固なハードウェアに記憶しても、ハードウェアを破壊する等の行為により、その情報を記憶する記憶媒体が奪取される場合が考えられる。この場合、記憶媒体を奪取した者を特定するため、ハードウェアを常時監視することが望ましい。

【０００５】

【発明が解決しようとする課題】上述したように、機密性の高いプログラムを有するコンピュータシステムでは、利用者のオペレーションが制限され、又、物理的に強固である特殊なハードウェアとそのハードウェアの監視とが必要とされていた。よって、パソコン等の汎用的なハードウェアを用いたシステムの構築は困難であった。また、ハードウェアの設置場所が常時監視可能な場所（例えば、監視カメラ又は係員による監視が可能な場所）に制限されていた。

【０００６】本発明は、上記実状に鑑みてなされたもので、セキュリティのレベルが高く、汎用的なハードウェアで実現可能なセキュリティシステム、機密プログラム管理方法及び記録媒体を提供することを目的とする。また、任意の場所に設置可能なセキュリティシステム、機密プログラム管理方法及び記録媒体を提供することを他の目的とする。

【０００７】

【課題を解決するための手段】上記目的を達成するため、この発明の第１の観点に係るセキュリティシステムは、サーバと、該サーバに接続された複数のクライアントと、を備えるクライアントサーバシステムにおいて、前記サーバは、機密情報を含む機密プログラムを記憶する機密プログラム記憶手段と、前記クライアントからの



要求に応じて、前記機密プログラム記憶手段に記憶されている前記機密プログラムを要求元の前記クライアントに送信する手段と、を備え、前記クライアントは、前記機密プログラムを前記サーバに要求する要求送信手段と、前記機密プログラムを受信する受信手段と、前記受信手段により受信された前記機密プログラムを記憶する記憶手段と、前記記憶手段により記憶された前記機密プログラムを実行する実行手段と、前記機密プログラム実行後、該機密プログラムを前記記憶手段から削除する削除手段と、を備える。

【０００８】このような構成によれば、機密性の高いプログラムをサーバで一元管理し、クライアントで機密プログラムを実行する必要が生じた場合のみ、そのクライアントに機密プログラムを転送し、転送先で機密プログラムの実行が完了した後、その転送先における機密プログラムを削除する。これにより、機密プログラムは、使用時のみクライアントに存在し、通常はクライアントに存在しない。よって、クライアントでは機密プログラムを常時格納するための特殊なハードウェアが不要となるため、クライアントを汎用的なハードウェアで構成することができる。

【０００９】前記クライアントは、前記機密プログラムへのアクセスに関する排他制御を行うロック制御手段と、前記記憶手段により前記機密プログラムが記憶された際に前記ロック制御手段に該機密プログラムへの排他制御を指示するロック指示手段と、前記実行手段による前記機密プログラムの実行終了後、前記ロック制御手段に該機密プログラムへの排他制御の解除を指示するロック解除指示手段と、を備えてもよく、前記クライアントの前記削除手段は、前記ロック解除指示手段による指示に応じて前記ロック制御手段により前記機密プログラムに関する排他制御が解除された後、該機密プログラムを前記記憶手段から削除する手段を備えてもよい。これにより、機密性の高い情報を含む機密プログラムがクライアントの記憶手段に記憶されている間、その機密プログラムに対してロックをかけることにより、第三者等によりいかなるオペレーションが行われようとも、機密プログラムへのアクセスを防ぐことができる。

【００１０】前記クライアントは、少なくとも前記ロック解除指示手段及び前記削除手段による一連の手続が完了するまでの間、タスクの切り替えを禁止する手段をさらに備えてもよい。

【００１１】前記クライアントは、前記削除手段による前記機密プログラムの削除後、該機密プログラムのファイル名と同一のファイル名のダミーファイルを作成して記憶するダミーファイル作成手段と、前記作成されたダミーファイルを削除するダミーファイル削除手段と、をさらに備えてもよい。これにより、機密性の高い情報を含む機密プログラムに対してロックをかけて第三者がアクセスできない状態でダミーファイルで上書きし、完全

に削除して復元不可能とすることにより、セキュリティをより高めることができる。

【００１２】前記クライアントは、少なくとも前記ロック解除指示手段、前記削除手段、前記ダミーファイル作成手段及び前記ダミーファイル削除手段による一連の手続が完了するまでの間、タスクの切り替えを禁止する手段をさらに備えてもよい。

【００１３】前記クライアントの前記削除手段は、前記機密プログラムの削除後、削除の完了を示す削除完了電文を前記サーバに送信する手段を備えてもよく、前記サーバは、前記機密プログラムの送信先の前記クライアントから前記削除完了電文を該機密プログラム送信時から所定時間内に受信したか否かを判別する判別手段と、前記削除完了電文を前記所定時間内に受信していないと判別された場合、不正検出を通知する手段と、を備えてもよい。

【００１４】このような構成によれば、機密プログラム送信時から所定時間内に、機密プログラムの転送先のクライアントから削除完了電文を受信したか否かを判別することにより、機密プログラムが奪取されたことを検知できる。

【００１５】前記クライアントは、該クライアントの利用者を特定する利用者情報を取得する取得手段を備えてもよく、前記クライアントの前記要求送信手段は、前記機密プログラムの要求を前記取得手段により取得された前記利用者情報と共に送信する手段を備えてもよく、前記サーバは、前記判別手段により、前記削除完了電文を前記所定時間内に受信しなかったと判別された場合、前記クライアントから受信した前記利用者情報から不正者を特定し、通知する手段を備えてもよい。

【００１６】このような構成によれば、機密プログラムが奪取された場合、利用者情報から不正者を特定することができる。よって、不正者を監視するためにクライアントの設置場所を限定することが不要となり、任意の場所にクライアントを設置することができる。

【００１７】また、この発明の第２の観点に係る機密プログラム管理方法は、機密プログラムを該機密プログラム保存用の第１の端末に格納するステップと、前記機密プログラムを実行する第２の端末に、前記第１の端末に記憶されている該機密プログラムを転送する転送ステップと、前記転送ステップにより前記機密プログラムが転送された前記第２の端末において、該機密プログラムを実行し、実行完了後、該機密プログラムを削除する削除ステップと、を備える。

【００１８】このような構成によれば、機密性の高いプログラムを第１の端末で一元管理し、第２の端末で機密プログラムを実行する場合のみ、その第２の端末に機密プログラムを転送し、転送先で機密プログラムの実行が完了した後、その転送先における機密プログラムを削除する。これにより、機密プログラムは、使用時のみ第２の端末に存在し、通常は存在しない。よって、第２の端末では機密プログラムを常時格納するための特殊なハードウェアを設ける必要がなくなり、第２の端末を汎用的なハードウェアで構成することができる。



【００１９】前記削除ステップにより前記機密プログラムが削除された後、削除の完了を前記第１の端末に通知する通知ステップと、前記第１の端末が、前記通知ステップによる削除の完了の通知を、前記転送ステップによる前記機密プログラムの転送時から所定時間内に受信したか否かを判別する判別ステップと、前記第１の端末が前記削除の完了の通知を前記所定時間内に受信していないと判別された場合、不正の検出を通知するステップと、を更に備えてもよい。

【００２０】このような構成によれば、機密プログラムの削除の完了の通知を転送先の第２の端末から機密プログラム送信時より所定時間内に受信したか否かを判別することにより、機密プログラムが不正に奪取されたことを検知することができる。

【００２１】該機密プログラム管理方法は、前記第２の端末に前記機密プログラムが記憶された際に、該機密プログラムへのアクセスに関する排他制御を行うロックステップと、前記第２の端末における前記機密プログラムの実行終了後、該機密プログラムへの排他制御を解除するロック解除ステップと、を備えてもよく、前記削除ステップは、前記ロック解除ステップにより前記機密プログラムに関する排他制御が解除された後、該機密プログラムを前記第２の端末から削除するステップを備えてもよい。

【００２２】また、該機密プログラム管理方法は、前記削除ステップによる前記機密プログラムの削除後、該機密プログラムのファイル名と同一のファイル名のダミーファイルを作成記憶するステップと、前記作成されたダミーファイルを削除するステップと、をさらに備えてもよい。

【００２３】前記転送ステップにより前記機密プログラムが転送された前記第２の端末において、該第２の端末の利用者を特定する利用者情報を取得する取得ステップと、前記取得ステップより取得された前記利用者情報を前記第１の端末に送信するステップと、前記判別ステップにより、前記第１の端末が前記機密プログラムの削除の完了の通知を前記所定時間内に受信していないと判別された場合、前記利用者情報から不正者を特定し、通知するステップと、を更に備えてもよい。

【００２４】このような構成によれば、機密プログラムが奪取された場合、利用者情報から不正者を特定することができる。よって、不正者を監視するために第２の端末の設置場所を限定することが不要となり、任意の場所に第２の端末を設置することができる。

【００２５】また、この発明の第３の観点に係る記録媒体は、コンピュータを、機密情報を含む機密プログラム

を要求する要求手段、前記機密プログラムを受信する受信手段、前記受信手段により受信された前記機密プログラムを記憶する記憶手段、前記記憶手段により記憶された前記機密プログラムを実行する実行手段、前記機密プログラム実行後、該機密プログラムを前記記憶手段から削除する削除手段、として機能させるためのプログラムを記録する。

【００２６】また、この発明の第４の観点に係る記録媒体は、コンピュータを、機密情報を含む機密プログラムを要求する要求手段、前記機密プログラムを受信する受信手段、前記受信手段により受信された前記機密プログラムを記憶する記憶手段、前記機密プログラムへのアクセスに関する排他制御を行うロック制御手段、前記記憶手段により前記機密プログラムが記憶された際に前記ロック制御手段に該機密プログラムへの排他制御を指示するロック指示手段、前記記憶手段により記憶された前記機密プログラムを実行する実行手段、前記実行手段による前記機密プログラムの実行終了後、前記ロック制御手段に該機密プログラムへの排他制御の解除を指示するロック解除指示手段、前記ロック解除指示手段による指示に応じて前記ロック制御手段により前記機密プログラムに関する排他制御が解除された後、該機密プログラムを前記記憶手段から削除する削除手段、として機能させるためのプログラムを記録する。

【００２７】また、この発明の第５の観点に係る記録媒体は、コンピュータを、機密情報を含む機密プログラムを要求する要求手段、前記機密プログラムを受信する受信手段、前記受信手段により受信された前記機密プログラムを記憶する記憶手段、前記機密プログラムへのアクセスに関する排他制御を行うロック制御手段、前記記憶手段により前記機密プログラムが記憶された際に前記ロック制御手段に該機密プログラムへの排他制御を指示するロック指示手段、前記記憶手段により記憶された前記機密プログラムを実行する実行手段、前記実行手段による前記機密プログラムの実行終了後、前記ロック制御手段に該機密プログラムへの排他制御の解除を指示するロック解除指示手段、前記ロック解除指示手段による指示に応じて前記ロック制御手段により前記機密プログラムに関する排他制御が解除された後、該機密プログラムを前記記憶手段から削除する削除手段、前記削除手段による前記機密プログラムの削除後、該機密プログラムのファイル名と同一のファイル名のダミーファイルを作成して記憶するダミーファイル作成手段、前記作成されたダミーファイルを削除するダミーファイル削除手段、として機能させるためのプログラムを記録する。

【００２８】

【発明の実施の形態】本発明の実施の形態にかかるセキュリティシステムについて、金銭的価値を有する電子マネーを格納するＩＣカード（電子マネーカード）を使用する電子マネーシステムを例に、以下図面を参照して説明する。この電子マネーシステムは、図１に示すように、サーバ１１と、カードリーダ／ライタ（以下、カードＲ／Ｗ）１３を備えるクライアント１５と、これらを接続するネットワーク１８と、電子マネーカード１９と、より構成される。

【００２９】サーバ１１の論理構成図（ソフトウェア構成図）を図２に示す。図示されるよに、サーバ１１は、通信制御プログラム２１と、ファイル転送プログラム２３と、ＩＣカード書込プログラム２５と、サーバプログラム２７と、ＯＳ（Operating System）２９と、を備える。

【００３０】通信制御プログラム２１は、外部と通信を行うための制御プログラムであり、例えばＴＣＰ／ＩＰプロトコル、ＬＡＮドライバ等から構成される。ファイル転送プログラム２３は、ファイルを転送するためのプログラムであり、例えばＦＴＰ（File Transfer Protocol）等から構成される。ＩＣカード書込プログラム２５は、電子マネーカード１９への書き込みを行うためのプログラムであり、書き込みを行う際に必要なパスワードを含む。サーバプログラム２７は、後述するクライアント１５のクライアントプログラムと通信するためのプログラムである。ＯＳ２９は、サーバ１１全体を管理するためのプログラムである。

【００３１】この電子マネーシステムにおける機密性の高い情報とは、例えば電子マネーカード１９にデータを書き込む為に必要なパスワードである。よって、この情報を有するＩＣカード書込プログラム２５が本システムにおける機密性の高いプログラムである。

【００３２】クライアント１５の論理構成図を図３に示す。図示されるように、クライアント１５は、通信制御プログラム３１と、ファイル転送プログラム３３と、クライアントプログラム３５と、ＩＣカードＲ／Ｗドライバ３７と、ＯＳ３９と、を備える。

【００３３】通信制御プログラム３１とファイル転送プログラム３３とＯＳ３９とは、上述したサーバ１１の通信制御プログラム２１とファイル転送プログラム２３とＯＳ２９とそれぞれ同等の機能を有するプログラムである。クライアントプログラム３５は、サーバプログラム２７との通信、サーバ１１からのファイル転送、クライアント１５に格納されているプログラムの起動、ＩＣカードＲ／Ｗドライバ３７を介した電子マネーカード１９とのデータの送受信、等を行うためのプログラムである。ＩＣカードＲ／Ｗドライバ３７は、カードＲ／Ｗ１３を制御するためのプログラムである。なお、本システムでは、電子マネーカード１９に書き込みをするためにはパスワードが必要であり、ＩＣカードＲ／Ｗドライバ３７は、このパスワードのチェック等も行う。

【００３４】サーバ１１のシステム構成図を図４に示す。図示されるように、サーバ１１は、ＣＰＵ４１と、メモリ４２と、入力装置４３と、表示装置４４と、補助

記憶装置４５と、通信制御装置４６と、を備える。図２を参照して上述したサーバ１１側のプログラムは、メモリ４２又は補助記憶装置４５に格納されており、例えばメモリ４２に常駐していないプログラムは、実行時に補助記憶装置４５からメモリ４２にロードされ、ＣＰＵ４１により実行される。通信制御部４６は、ＣＰＵ４１からの指示により、クライアント１５との通信を行う。

【００３５】クライアント１５のシステム構成図を図５に示す。図示されるように、クライアント１５は、ＣＰＵ５１と、メモリ５２と、入力装置５３と、表示装置５４と、補助記憶装置５５と、通信制御装置５６と、ＩＣカードＲ／Ｗ制御装置５７と、を備える端末である。クライアント１５は、カードＲ／Ｗ１３とクライアント１５を接続し、カードＲ／Ｗ１３を制御するためのＩＣカードＲ／Ｗ制御装置５７を備える点以外は、上述したサーバ１１と同様の構成を有する。

【００３６】電子マネーカード１９は、図６に示すように、その電子マネーカード１９の保有者の情報である利用者情報と、その電子マネーカード１９の利用履歴と、残高を記憶する。利用者情報は、利用者ＩＤ、氏名、住所、電話番号等を含む。

【００３７】この電子マネーシステムは、電子マネーカード１９にデータを書き込むためのパスワードを含むＩＣカード書込プログラム２５を、サーバ１１のみに格納する。そして、クライアント１５でそのプログラムを実行する必要が生じた際に、サーバ１１から転送し、実行終了後、プログラムをクライアント１５から削除することにより、高レベルのセキュリティを保持する。ＩＣカード書込プログラム２５をサーバ１１からクライアント１５に転送し、転送したプログラムの実行完了後、そのプログラムを消去する機密プログラム転送処理について図７、図８を参照して説明する。

【００３８】まず、クライアント１５での処理を図７のフローチャートを用いて説明する。利用者により電子マネーの取引の指示がクライアント１５に入力され、この入力に応答し、クライアントプログラム３５が利用者の電子マネーカード１９に記憶されている利用者を特定する情報（利用者情報）をＩＣカードＲ／Ｗドライバ３７を介して読み出す（ステップＳ１）。次に、クライアントプログラム３５は、読み出した利用者情報を、通信制御プログラム３１を介してサーバ１１に送信する（ステップＳ２）。

【００３９】送信した利用者情報に応答してサーバ１１から送信されたＩＣカード書込プログラム２５を、ファイル転送プログラム３３が通信制御プログラム３１を介して受信し、クライアントプログラム３５に渡す（ステップＳ３）。クライアントプログラム３５は、受信したＩＣカード書込プログラム２５を実行する（ステップＳ４）。実行終了後、クライアントプログラム３５は、ＩＣカード書込プログラム２５を削除し（ステップＳ５）、機密プログラムの削除の完了を示す削除完了電文を通信制御プログラム３１を介してサーバ１１に送信する（ステップＳ６）。

【００４０】次に、サーバ１１での処理を図８のフローチャートを用いて説明する。サーバ１１の通信制御プログラム２１は、クライアント１５からの利用者情報を受信し、サーバプログラム２７に渡す（ステップＳ１１）。サーバプログラム２７は、利用者情報を受信すると、ＩＣカード書込プログラム２５をクライアント１５へ送信するようファイル転送プログラム２３に指示する。この指示に応答して、ファイル転送プログラム２３は、ＩＣカード書込プログラム２５を通信制御プログラム２１を介してクライアント１５に転送する（ステップＳ１２）。

【００４１】サーバプログラム２７は、ＩＣカード書込プログラム２５をクライアント１５に転送した後、そのクライアント１５からの削除完了電文を所定時間待つ（ステップＳ１３）。所定時間内にクライアント１５から削除完了電文を受信した場合、処理を終了する。所定時間が経過しても、クライアント１５から削除完了電文が到着しない場合、機密プログラムが奪取された等、不正検出の旨のエラーメッセージを表示する。また、サーバプログラム２７は、今回の処理においてクライアント１５から受信した利用者情報から不正者を特定し、管理者等に通知する（ステップＳ１４）。

【００４２】上述のように、機密性の高いＩＣカード書込プログラム２５をサーバ１１からクライアント１５に転送し、使用後に削除することにより、ＩＣカード書込プログラム２５をクライアント１５に常駐させなくてもよい。このため、クライアント１５のハードウェアを強化したり、利用者のオペレーションを限定する必要がなくなる。また、機密性の高いプログラムがクライアント１５に格納されている間に、そのプログラムが記憶されているハードウェアが利用者により奪取された場合は、削除完了電文がサーバ１１に返らないことから、その不正を検知することができる。また、不正を検出した場合、サーバ１１は、クライアント１５から受信した利用者情報により、不正者を特定することができる。

【００４３】次に、この電子マネーシステムで、利用者Ａが自己の電子マネーカード１９を用いて、クライアント１５Ｂで買い物をする場合について、図９を参照して説明する。なお、この電子マネーシステムでは、利用者がクライアント１５Ｂの表示装置５４に表示された物品の中から、購入したい物品を入力装置５３より入力し、入力された物品が、後日、利用者に発送されることとする。

【００４４】利用者Ａは、自己の電子マネーカード１９をクライアント１５Ｂに接続されているカードＲ／Ｗ１３に装着し、表示装置５４に表示されている物品の中から所望の物品を選択し、入力装置５３から購入要求を入

力する。クライアント１５Ｂのクライアントプログラム３５は、この購入要求に応答し、ＩＣカードＲ／Ｗドライバ３７を介して、カードＲ／Ｗ１３に装着されている電子マネーカード１９から利用者Ａの利用者情報を読み出す（図９（Ａ）Ｐ１）。次に、クライアントプログラム３５は、読み出した利用者情報を、通信制御プログラム３１を介してサーバ１１に送信する（Ｐ２）。

【００４５】サーバ１１の通信制御プログラム２１は、クライアント１５Ｂから利用者情報を受信し、サーバプログラム２７に送る。サーバプログラム２７は、通信制御プログラム２１からの利用者情報に応答して、クライアント１５ＢへＩＣカード書込プログラム２５を転送するようファイル転送プログラム２３に指示する（図９（Ｂ）Ｐ３）。ファイル転送プログラム２３は、この指示に応答し、ＩＣカード書込プログラム２５を通信制御プログラム２１を介してクライアント１５Ｂに転送する（Ｐ４）。サーバプログラム２７は、ＩＣカード書込プログラム２５の送信後、所定時間（例えば、５分間）、クライアント１５Ｂからの削除完了電文を待つ。

【００４６】クライアント１５Ｂのファイル転送プログラム３３は、通信制御プログラム３１を介してＩＣカード書込プログラム２５を受信し、クライアントプログラム３５に渡す。クライアントプログラム３５は、ＩＣカード書込プログラム２５を起動する。起動されたＩＣカード書込プログラム２５は、自己が有するパスワードを用いて、ＩＣカードＲ／Ｗドライバ３７を介してＩＣカードにアクセスする。ＩＣカード書込プログラム２５は、電子マネーカード１９の利用履歴として利用者Ａが購入した物品の情報（例えば、物品を特定するためのコード、価格、購入日等）を書き込み、その電子マネーカードに記憶されている電子マネーの残高から物品の価格を差し引く（図９（Ｃ）Ｐ５）。

【００４７】ＩＣカード書込プログラム２５の処理（電子マネーカード１９への書き込み）が終了すると、クライアントプログラム３５は、ＩＣカード書込プログラム２５を削除し（図９（Ｄ）Ｐ６）、プログラムの削除の完了を示す削除完了電文を通信制御プログラム３１を介してサーバ１１に送信する（Ｐ７）。また、クライアントプログラム３５は、ＩＣカードＲ／Ｗドライバ３７を介して、カードＲ／Ｗ１３に装着された電子マネーカード１９を排出する。サーバプログラム２７は、クライアント１５Ｂから削除完了電文を受信し、処理を終了する。

【００４８】また、ＩＣカード書込プログラム２５がクライアント１５Ｂに存在している間に、利用者Ａがクライアント１５Ｂ全体又はＩＣカード書込プログラム２５が記憶されている補助記憶装置５５を奪取する等の不正を行った場合（図９（Ｅ）Ｐ８）、クライアント１５Ｂは削除完了電文をサーバ１１に送信しない。この場合、サーバ１１のサーバプログラム２７は削除完了電文を受信しないため、所定時間経過後、不正検出のメッセージを表示装置４４に表示すると共に、クライアント１５Ｂから受信した利用者情報より不正者が利用者Ａであると特定し、その旨を表示する（Ｐ９）。

【００４９】このようにして、ＩＣカード書込プログラム２５をサーバ１１からクライアント１５Ｂに転送し、使用後に削除することにより、クライアント１５Ｂ上でＩＣカード書込プログラム２５を安全に動作させることができる。また、ＩＣカード書込プログラム２５がクライアント１５Ｂに格納されている間に奪取された場合には、クライアント１５Ｂから受信した利用者情報により、不正者を特定することができる。

【００５０】なお、クライアント１５が、サーバ１１から上記ＩＣカード書込プログラム２５等の機密プログラムをファイル転送により受け取り、自己の記憶領域に記憶した際に、その機密プログラムに対してファイルロックをかけ、クライアントプログラム３５以外からアクセスできないようして、セキュリティを強化してもよい。この場合のクライアント１５Ｃは、図１０に示すように、上記クライアントプログラム３５にファイルロック機能を追加したクライアントプログラム３５Ｃを有する点以外は、上記クライアント１５とほぼ同様の構成を有する。以下、このクライアント１５Ｃの動作について図１１のフローチャートを参照して説明する。

【００５１】クライアント１５Ｃは、例えば利用者による指示に応答し、利用者の電子マネーカード１９の利用者情報をＩＣカードＲ／Ｗドライバ３７を介して読み出し、該利用者情報を通信制御プログラム３１を介してサーバ１１に送信する（ステップＳ１１）。送信した利用者情報に応答してサーバ１１から送信されたＩＣカード書込プログラム２５をファイル転送プログラム３３が通信制御プログラム３１を介して受信し、クライアントプログラム３５Ｃに渡す（ステップＳ１２）。これにより、ＩＣカード書込プログラム２５のファイルがクライアント１５Ｃのハードディスクに作成される。

【００５２】次に、クライアントプログラム３５Ｃが、ＩＣカード書込プログラム２５のファイルに対しファイルロックをかけるよう指示するファイルロックコマンドをＯＳ３９に発行して、ＩＣカード書込プログラム２５のファイルをファイルロックする（ステップＳ１３）。これにより、ＩＣカード書込プログラム２５は、クライアントプログラム３５Ｃ以外からアクセスできなくなる。この状態でクライアントプログラム３５ＣはＩＣカード書込プログラム２５を実行する（ステップＳ１４）。実行終了後、クライアントプログラム３５Ｃは、クライアント１５Ｃ上で他のタスクが実行されないようにＯＳ３９にタスク切替禁止コマンドを発行し、タスクの切り替えを禁止する（ステップＳ１５）。

【００５３】コマンド発行後、クライアントプログラム３５Ｃは、ＩＣカード書込プログラム２５のファイルロ

ックを解除するためのファイルロック解除コマンドをＯＳ３９に発行し、ＩＣカード書込プログラム２５に対するファイルロックを解除する（ステップＳ１６）。次に、クライアントプログラム３５Ｃは、ＩＣカード書込プログラム２５を削除するための削除コマンドをＯＳ３９に発行し、ＩＣカード書込プログラム２５を削除する（ステップＳ１７）。削除コマンド発行後、クライアントプログラム３５Ｃは、ステップＳ１５で発行したタスク切替禁止コマンドを解除するための解除コマンドをＯＳ３９に発行して、タスクの切り替えの禁止を解除し（ステップＳ１８）、機密プログラムの削除の完了を示す削除完了電文を通信制御プログラム３１を介してサーバ１１に送信し（ステップＳ１９）、処理を終了する。

【００５４】このようにして、ＩＣカード書込プログラム２５等の機密性の高い情報を含むプログラムがクライアント１５Ｃに格納されている間は、その機密プログラムに対してロックをかけることにより、第三者（利用者を含む）によりいかなるオペレーションが行われようとも、機密プログラムへのアクセスを防ぐことができる。なお、この場合のサーバ１１の構成及び動作は上記と同様である。

【００５５】また、上記クライアント１５Ｃにおいて機密プログラムを削除した場合、ＦＡＴ（File Access Table）上では、機密プログラムは削除されているが、記憶ディスクにはその機密プログラムが残存している。この記憶ディスクに残存している機密プログラムに任意情報を上書きして完全に削除することにより、さらにセキュリティを強化してもよい。この場合のクライアント１５Ｄは、図１２に示すように、上記クライアントプログラム３５Ｃに、上書きによる削除機能を追加したクライアントプログラム３５Ｄを有する点以外は、上記クライアント１５Ｃとほぼ同様の構成を有する。以下、このクライアント１５Ｄの動作について図１３のフローチャートを参照して説明する。

【００５６】クライアント１５Ｄは、例えば利用者による指示に応答し、利用者の電子マネーカード１９の利用者情報をＩＣカードＲ／Ｗドライバ３７を介して読み出し、該利用者情報を通信制御プログラム３１を介してサーバ１１に送信する（ステップＳ２１）。送信した利用者情報に応答してサーバ１１から送信されたＩＣカード書込プログラム２５をファイル転送プログラム３３が通信制御プログラム３１を介して受信し、クライアントプログラム３５Ｄに渡す（ステップＳ２２）。これにより、ＩＣカード書込プログラム２５のファイルがクライアント１５Ｄのハードディスクに作成される。

【００５７】次に、クライアントプログラム３５Ｄが、ＩＣカード書込プログラム２５に対するファイルロックコマンドを発行し（ステップＳ２３）、ＩＣカード書込プログラム２５を実行する（ステップＳ２４）。実行終了後、クライアントプログラム３５Ｄは、タスク切替禁止コマンドを発行して、タスクの切り替えを禁止する（ステップＳ２５）。これにより、例えば第三者がＩＣカード書込プログラム２５に別のプログラムからアクセスしようとしてもできなくなる。

【００５８】コマンド発行後、クライアントプログラム３５Ｄは、ＩＣカード書込プログラム２５のファイルに対するファイルロック解除コマンドを発行し（ステップＳ２６）、ＩＣカード書込プログラム２５を削除するための削除コマンドを発行する（ステップＳ２７）。この時点では、ＦＡＴ上ではＩＣカード書込プログラム２５のファイルが削除されたこととなるが、ＩＣカード書込プログラム２５のファイル自体は記憶ディスクから未だ削除されていない。

【００５９】削除コマンド発行後、クライアントプログラム３５Ｄは、ＩＣカード書込プログラム２５のファイルと同一のファイル名のダミーファイルを作成し記憶する（ステップＳ２８）。これにより、記憶ディスクにおけるＩＣカード書込プログラム２５は、新規に作成された同一ファイル名のダミーファイルにより上書きされるため、ＩＣカード書込プログラム２５はハードディスクから完全に削除される。なお、ダミーファイルの内容は任意であり、例えば空白文字からなる１０００バイトのファイルとしてもよい。ダミーファイル作成後、クライアントプログラム３５Ｄは、そのダミーファイルを削除する削除コマンドを発行する（ステップＳ２９）。ステップＳ２９における削除コマンド実行後においても、ハードディスクにはダミーファイルが残存しているが、仮にそのダミーファイルを第三者に見られたとしても問題ない。

【００６０】次に、クライアントプログラム３５Ｄは、タスクの切り替えの禁止を解除するための解除コマンドを発行して（ステップＳ３０）、処理を終了する。なお、必要に応じて、ステップＳ２９の後で、機密プログラムの削除の完了を示す削除完了電文を通信制御プログラム３１を介してサーバ１１に送信してもよい。

【００６１】このようにして、ＩＣカード書込プログラム２５等の機密性の高い情報を含むプログラムをクライアント１５Ｄに転送した際、その機密プログラムに対してロックをかけて第三者がアクセスできない状態で、ハードディスク上でダミーファイルで上書きして完全に削除して復元不可能とすることにより、セキュリティをより高めることができる。なお、この場合のサーバ１１の構成及び動作は上記と同様である。

【００６２】なお、この発明は、電子マネーシステムに限定されず、機密性の高い情報を有するプログラムを実行する任意のコンピュータシステムに適用可能である。例えば、特定の社員だけが機密の回覧を見ることができる回覧システムとして実現してもよい。このシステムでは、例えば、回覧データにアクセスするためにはパスワードが必要であり、そのパスワードを含み、回覧データ

を表示する回覧表示プログラムがサーバに格納されている。社員がクライアントに入力した社員ＩＤがサーバに送信され、サーバが、登録された社員ＩＤか否かを判別し、登録されている場合、回覧表示プログラムをクライアントに転送し、実行後、削除するようにしてもよい。

【００６３】サーバが乱数を生成し、機密プログラムと併せてクライアントに転送し、クライアントが、サーバから受信した乱数を削除完了電文に含めて送信するようにしてもよい。これにより、削除完了電文の偽造が困難となるため、機密プログラムを奪取した不正者が削除完了電文を偽造してサーバに送信することを防止することができる。また、サーバが暗号鍵を機密プログラムと共にクライアントに送信し、クライアントが、受信した暗号鍵で削除完了電文を暗号化して送信するようにしてもよい。

【００６４】サーバ、クライアント間の通信を、ＲＳＡ方式等を用いて暗号化してもよい。

【００６５】なお、機密プログラムを機密プログラム保存用の端末に格納しておき、要求に応じて、その機密プログラム保存用の端末から要求元のクライアント（端末）に機密プログラムを転送するようにしてもよい。

【００６６】また、上記説明におけるサーバ１１及びクライアント１５の論理構成は一例であり、これに限定されない。

【００６７】なお、上述説明における通信制御プログラム２１、ファイル転送プログラム２３、ＩＣカード書込プログラム２５、サーバプログラム２７を格納した媒体（フロッピーディスク、ＣＤ－ＲＯＭ等）から該プログラムをインストールすることにより、上記サーバ１１を実現してもよい。また、通信制御プログラム３１、ファイル転送プログラム３３、クライアントプログラム３５を格納した媒体から該プログラムをインストールすることにより、上記クライアント１５を実現してもよい。また、コンピュータに上記プログラムを供給するための媒体は、通信媒体（通信回線、通信ネットワーク、通信システムのように、一時的且つ流動的にプログラムを保持する媒体）でも良い。例えば、通信ネットワークの掲示板（ＢＢＳ）に該プログラムを掲示し、これをネットワークを介して配信してもよい。

【００６８】

【発明の効果】以上説明したように、本発明によれば、機密性の高いプログラムをサーバで一元管理し、クライアントで実行する必要が生じた場合のみ、機密プログラムを転送し、機密プログラムの実行が完了した後、クライアントにおける機密プログラムを削除する。これにより、機密プログラムは、使用時のみクライアントに存在＊し、通常はクライアントに存在しない。よって、クライアントでは機密プログラムを常時格納するための特殊なハードウェアを設ける必要がなく、クライアントを汎用的なハードウェアで構成することができる。また、機密プログラムが奪取された場合、利用者情報から不正者を特定することができるため、不正者を監視するためにクライアントの設置場所を限定することが不要となり、任意の場所にクライアントを設置することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係る電子マネーシステムの構成を示す図である。

【図２】サーバの論理的構成を示す図である。

【図３】クライアントの論理的構成を示す図である。

【図４】サーバのシステム構成を示す図である。

【図５】クライアントのシステム構成を示す図である。

【図６】電子マネーカードに記憶されるデータの構造を示す図である。

【図７】クライアントにおける機密プログラム転送処理を説明するためのフローチャートである。

【図８】サーバにおける機密プログラム転送処理を説明するためのフローチャートである。

【図９】この電子マネーシステムにおける機密プログラム転送処理を具体的に説明するための図である。

【図１０】ファイルロック機能を有する場合のクライアントの論理的構成を示す図である。

【図１１】図１０に示すクライアントにおける機密プログラム転送処理を説明するためのフローチャートである。

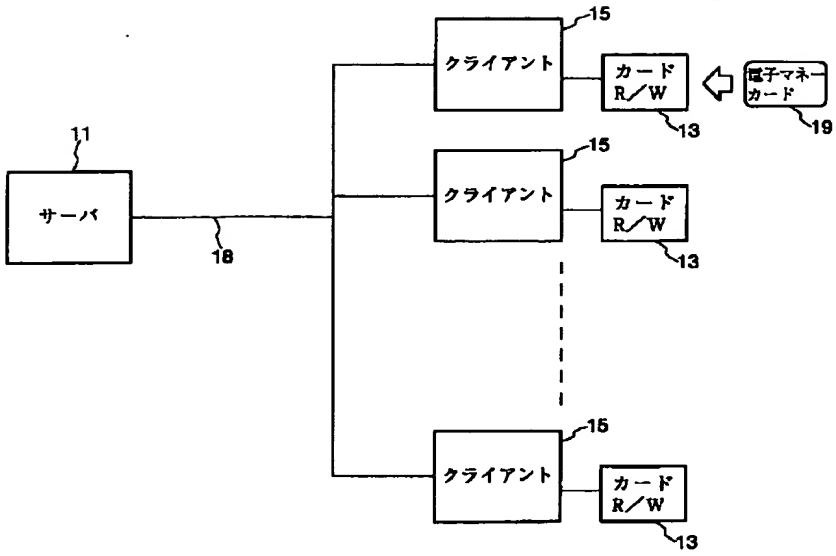
【図１２】上書きによるファイル削除機能を有する場合のクライアントの論理的構成を示す図である。

【図１３】図１２に示すクライアントにおける機密プログラム転送処理を説明するためのフローチャートである。

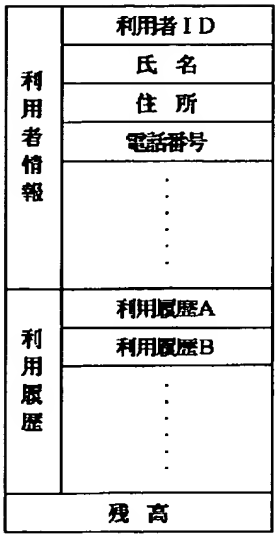
【符号の説明】

１１　　サーバ
１３　　カードＲ／Ｗ
１５、１５Ｃ、１５Ｄ　　クライアント
１８　　ネットワーク
１９　　電子マネーカード
２１、３１　　通信制御プログラム
２３、３３　　ファイル転送プログラム
２５　　ＩＣカード書込プログラム
２７　　サーバプログラム
２９、３９　　ＯＳ
３５、３５Ｃ、３５Ｄ　　クライアントプログラム
３７　　ＩＣカードＲ／Ｗドライバ

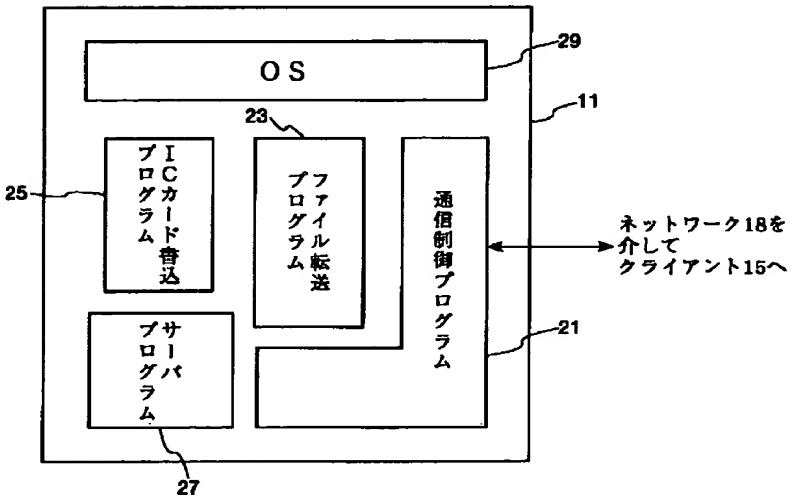
【図１】


11
サーバ
18
クライアント
15
カード R／W
13
電子マネーカード
19
クライアント
15
カード R／W
13
クライアント
15
カード R／W
13

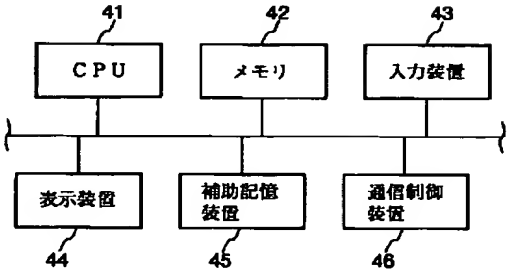
【図６】


利用者情報
利用者ＩＤ
氏　名
住　所
電話番号
利用履歴
利用履歴A
利用履歴B
残　高

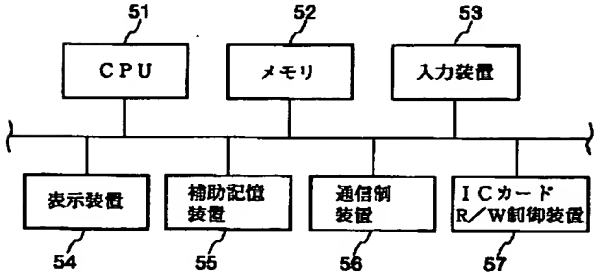
【図２】


ＯＳ
29
11
23
25
ＩＣカード書込プログラム
ファイル転送プログラム
通信制御プログラム
21
サーバプログラム
27
ネットワーク18を介してクライアント15へ

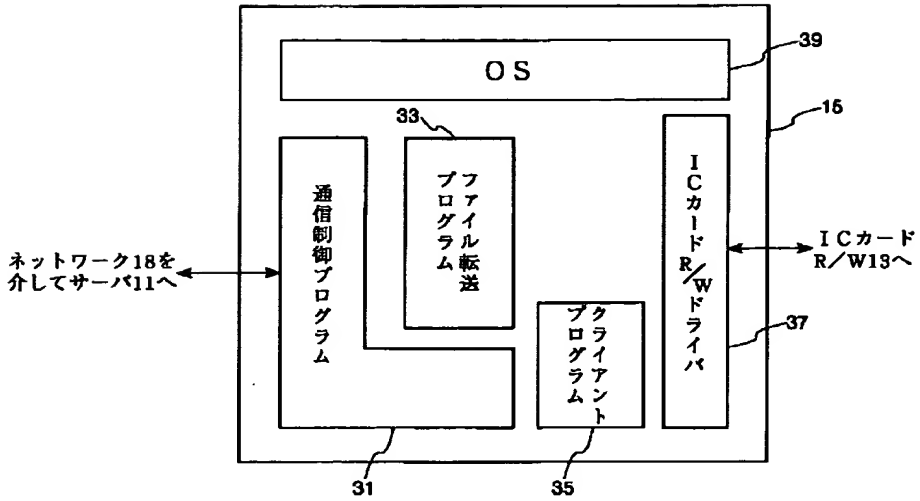
【図４】


41
CPU
42
メモリ
43
入力装置
表示装置
44
補助記憶装置
45
通信制御装置
46

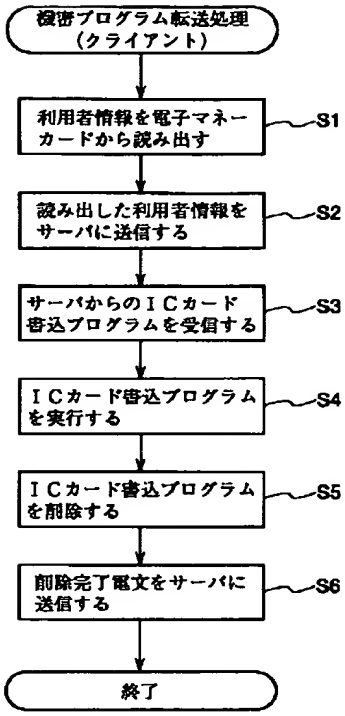
【図５】


51
CPU
52
メモリ
53
入力装置
表示装置
54
補助記憶装置
55
通信制装置
56
ＩＣカードR／W制御装置
57

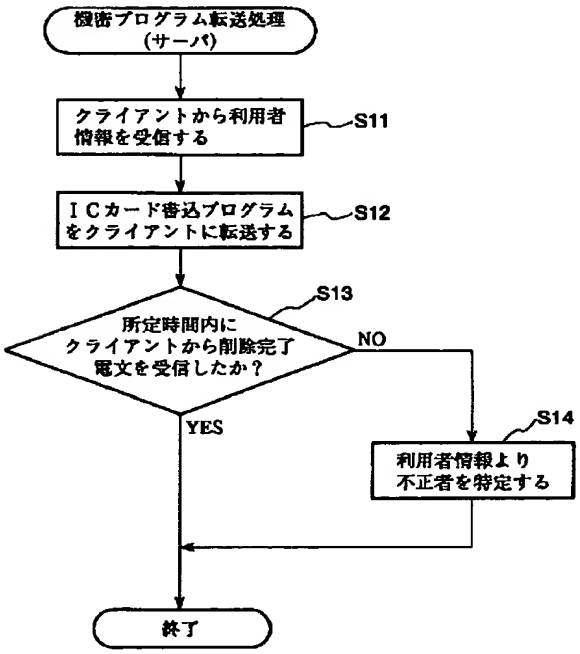
【図３】


ＯＳ
39
15
33
通信制御プログラム
ファイル転送プログラム
クライアントプログラム
ＩＣカードR/Wドライバ
37
ネットワーク18を介してサーバ11へ
ＩＣカードR/W13へ
31
35

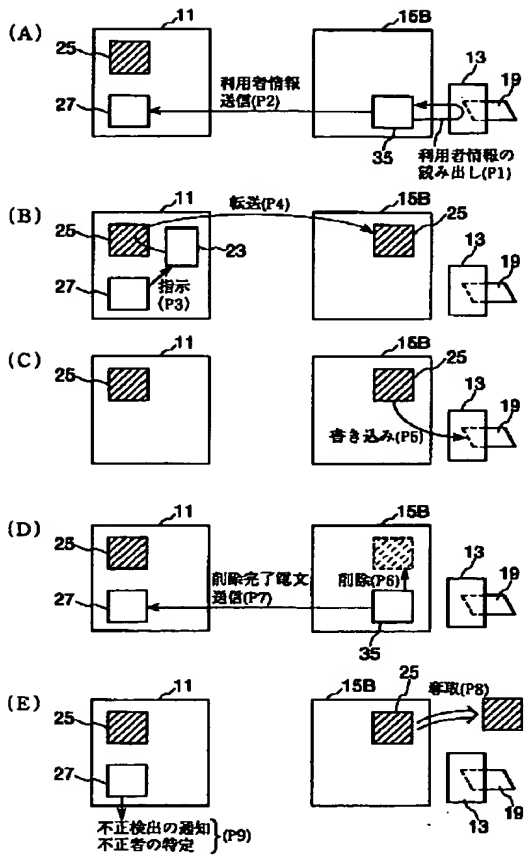
【図７】


機密プログラム転送処理（クライアント）
利用者情報を電子マネーカードから読み出す
S1
読み出した利用者情報をサーバに送信する
S2
サーバからのＩＣカード書込プログラムを受信する
S3
ＩＣカード書込プログラムを実行する
S4
ＩＣカード書込プログラムを削除する
S5
削除完了電文をサーバに送信する
S6
終了

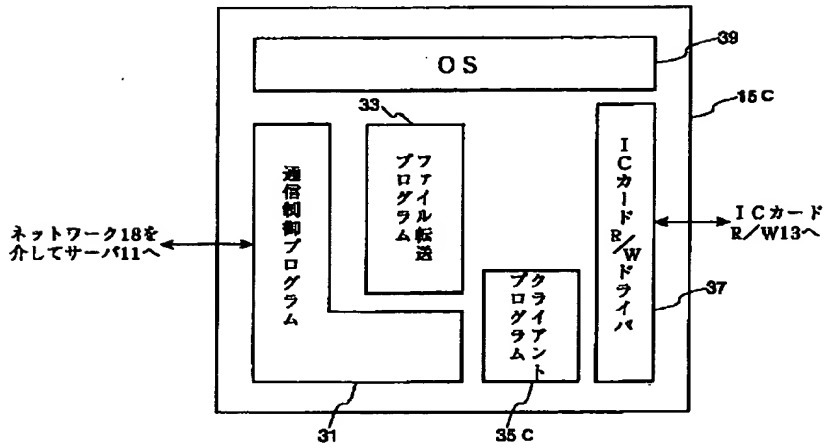
【図８】


機密プログラム転送処理（サーバ）
クライアントから利用者情報を受信する
S11
ＩＣカード書込プログラムをクライアントに転送する
S12
S13
所定時間内にクライアントから削除完了電文を受信したか？
NO
YES
S14
利用者情報より不正者を特定する
終了

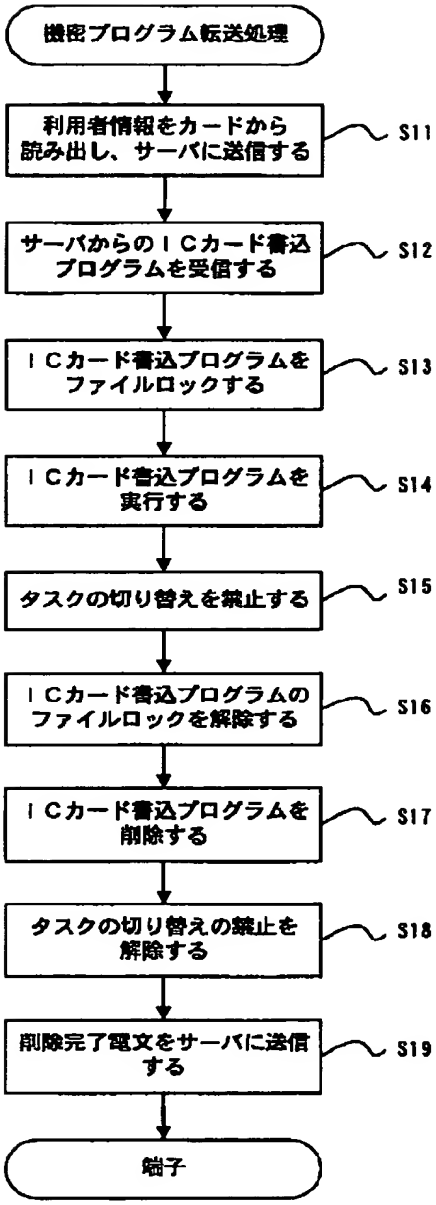
【図９】


(A)
11
25
27
利用者情報
送信(P2)
15B
13
19
35
利用者情報の
読み出し(P1)
(B)
転送(P4)
23
指示
(P3)
(C)
書き込み(P5)
(D)
削除完了電文
送信(P7)
削除(P6)
(E)
奪取(P8)
不正検出の通知
不正者の特定
(P9)

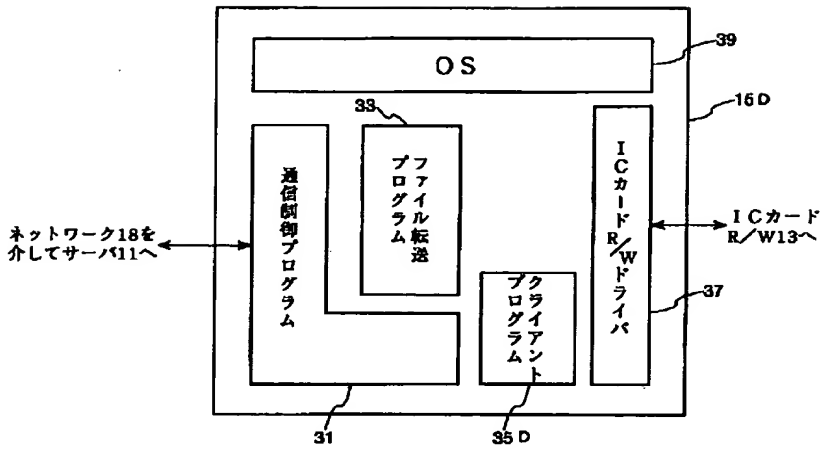
【図１０】


OS
39
15C
33
通信制御プログラム
ファイル転送プログラム
クライアントプログラム
ICカードR/Wドライバ
37
ネットワーク18を
介してサーバ11へ
ICカード
R/W13へ
31
35C

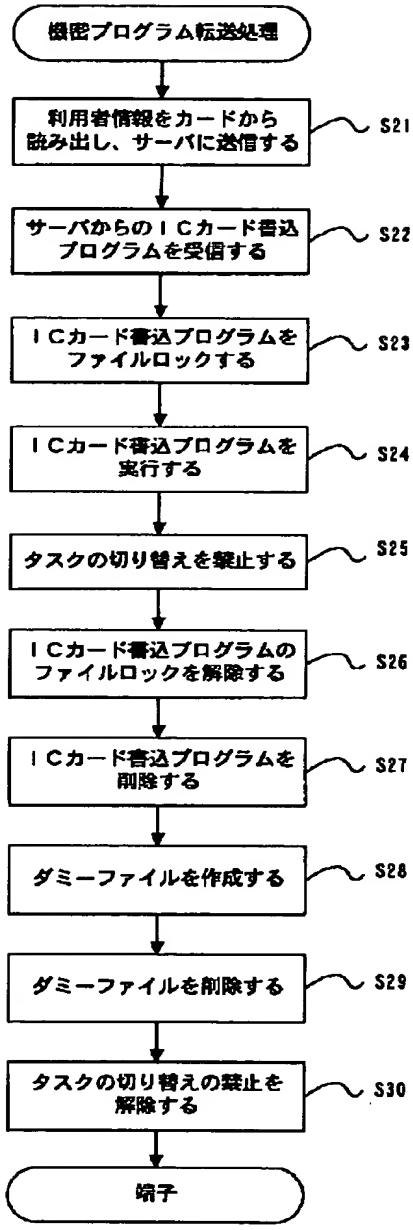
【図１１】


機密プログラム転送処理
利用者情報をカードから読み出し、サーバに送信する
S11
サーバからのＩＣカード書込プログラムを受信する
S12
ＩＣカード書込プログラムをファイルロックする
S13
ＩＣカード書込プログラムを実行する
S14
タスクの切り替えを禁止する
S15
ＩＣカード書込プログラムのファイルロックを解除する
S16
ＩＣカード書込プログラムを削除する
S17
タスクの切り替えの禁止を解除する
S18
削除完了電文をサーバに送信する
S19
端子

【図１２】


OS
39
16D
33
ファイル転送プログラム
通信制御プログラム
クライアントプログラム
ICカードR/Wドライバ
37
ネットワーク18を介してサーバ11へ
ICカードR/W13へ
31
35D

【図１３】


機密プログラム転送処理
利用者情報をカードから読み出し、サーバに送信する
S21
サーバからのICカード書込プログラムを受信する
S22
ICカード書込プログラムをファイルロックする
S23
ICカード書込プログラムを実行する
S24
タスクの切り替えを禁止する
S25
ICカード書込プログラムのファイルロックを解除する
S26
ICカード書込プログラムを削除する
S27
ダミーファイルを作成する
S28
ダミーファイルを削除する
S29
タスクの切り替えの禁止を解除する
S30
端子